Атака на потоковый шифр

- Ошибка: использование одинаковой шифрующей последовательности.
- 1-й сеанс: шифрование сообщения M_1
  - $E_1=M_1+\gamma$;
- 2-й сеанс: шифрование сообщения M_1
  - $E_2=M_2+\gamma$;

- Противник получает из лини связи: E_1 E_2

Действия противника:

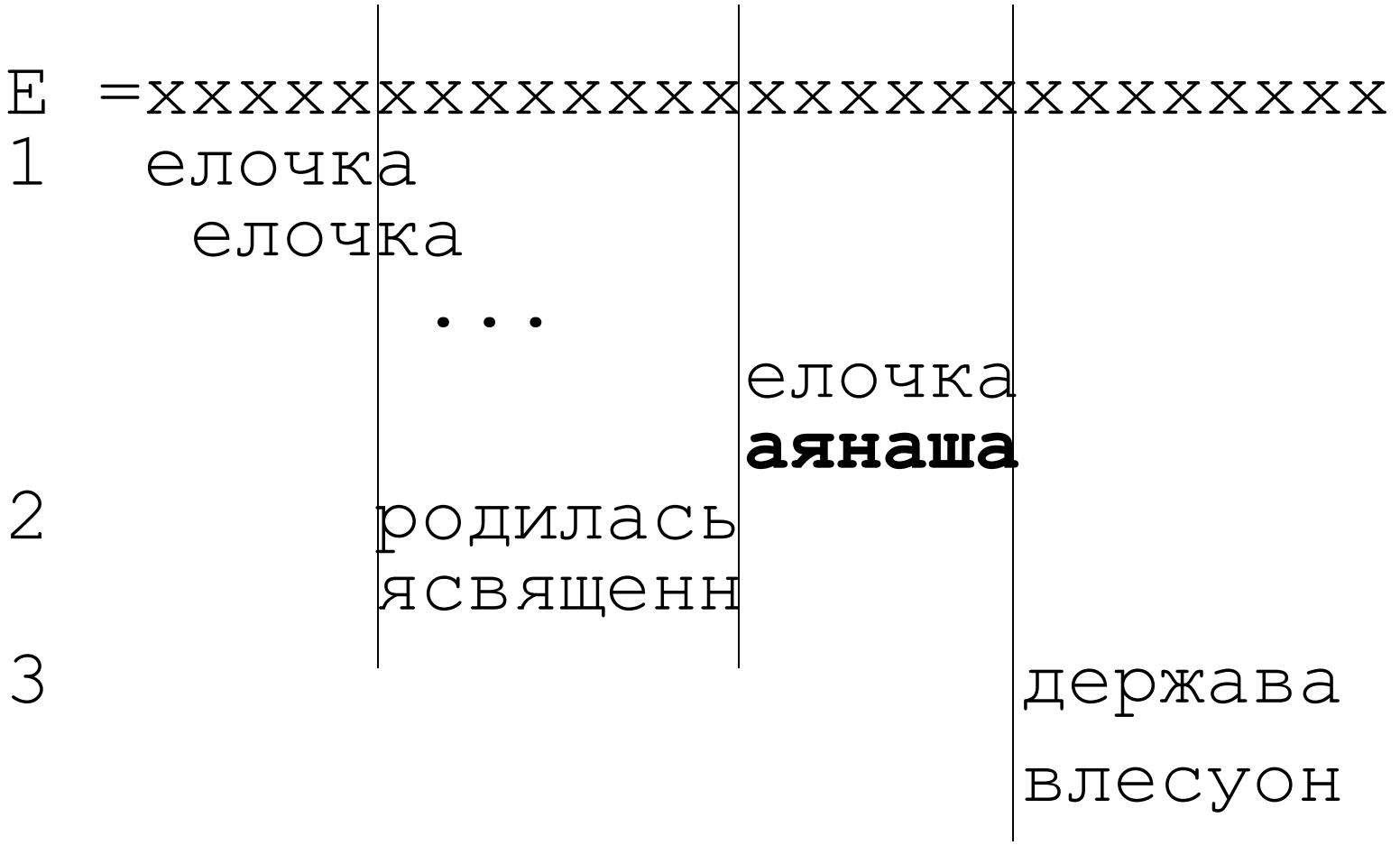
- $E_1 + E_2 = M_1 + \gamma + M_2 + \gamma = M_1 + M_2$;
  - Т.о. Противник свел потоковый шифр к книжному (один осмысленный текст шифруется другим осмысленным текстом).

Подход к вскрытию книжного шифра

```
M1=влесуродиласьелочкавлесуона
M2=россиясвященнаянашадержавар
E =xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Для вскрытия может использоваться частотный словарь словоформ русского языка (для другого типа данных аналогичный словарь надо составлять самостоятельно).

Перебор слов

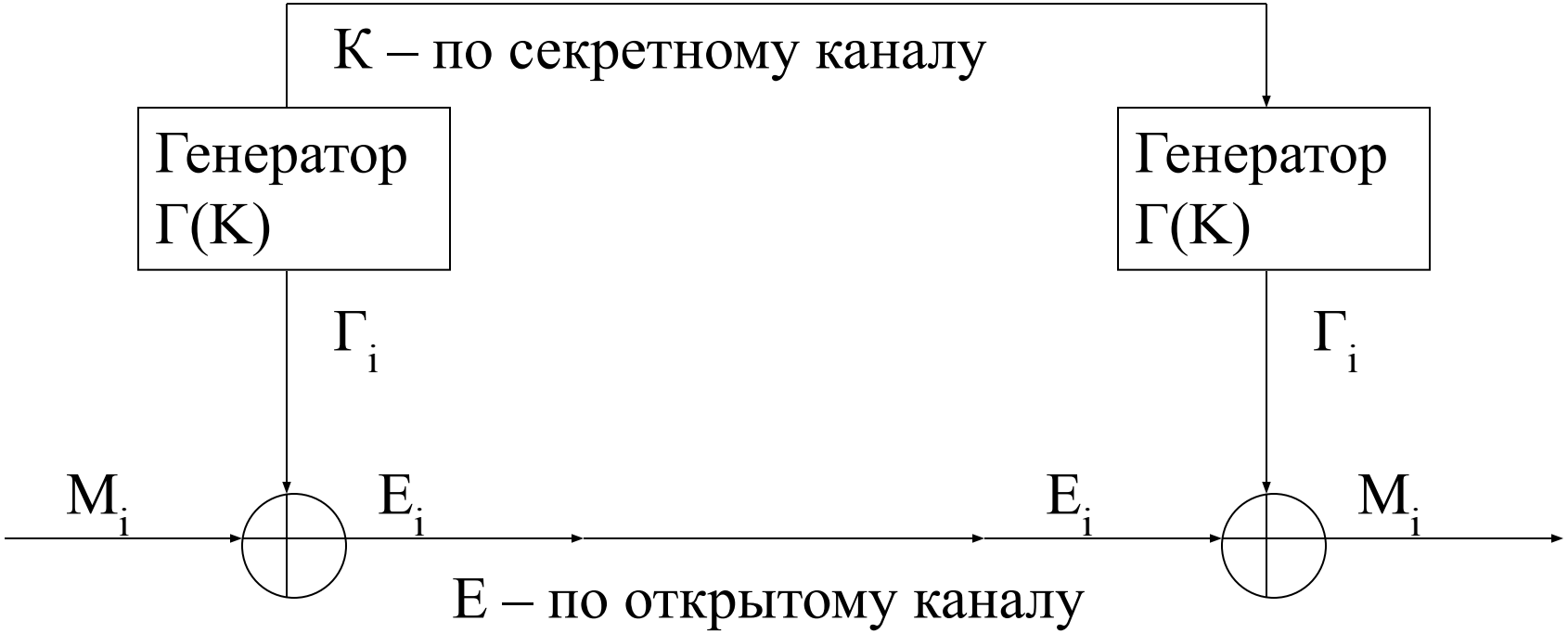


Потоковые шифры

- Посимвольное шифрование.
- Каждый символ сообщения (независимо от других) преобразуется в символ криптограммы по правилу, определяемому ключом. Ключ меняется от символа к символу.

  - Исторически первое применение –Вернам для телеграфных линий.

Потоковое шифрование



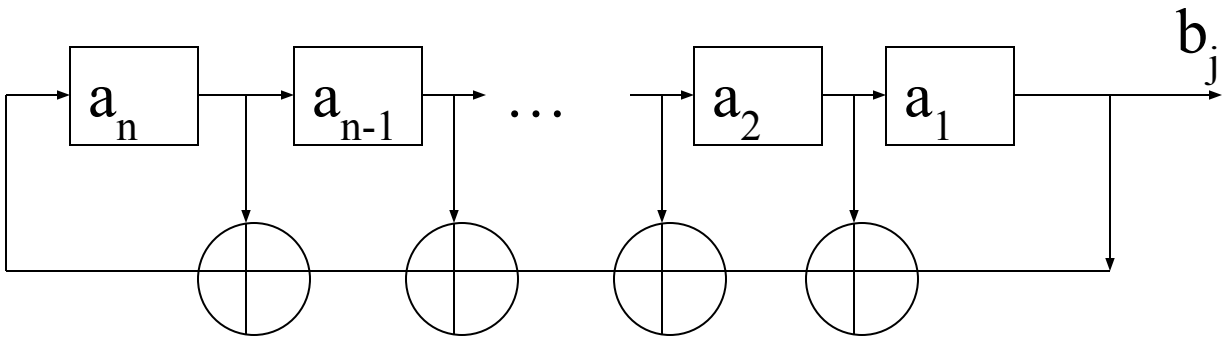
Г – шифрующая последовательность

Потоковые шифры

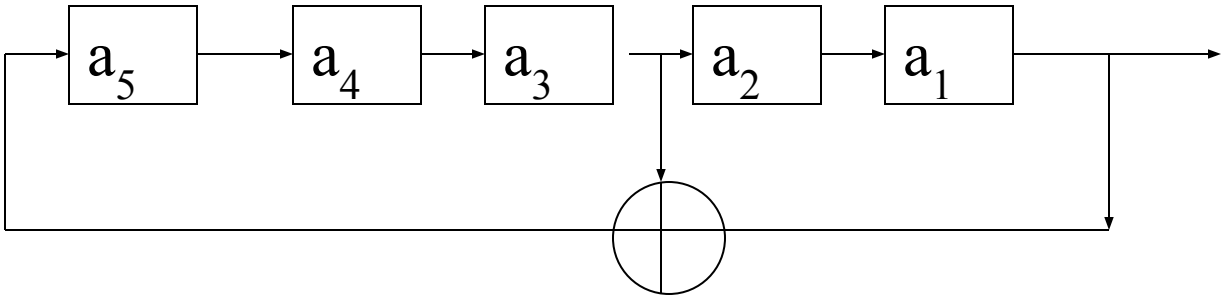
- Большинство потоковых шифров – аддитивные (шифрование по модулю 2)
- Отличаются друг от друга принципом формирования шифрующей последовательности

LSFR

- Для формирования последовательности часто используют:
  - ЛРР линейные рекуррентные регистры или иначе LSFR (регистры сдвига с линейными обратными связями).



LSFR



С любым ЛРР(LFSR) можно сопоставить полином обратных связей (для математического изучения свойств ЛРР):

$$h(x)=x^n+k_{n-1}x^{n-1}+k_2x^2+k_1x+1,$$

k_i-двоичные коэффициенты, определяющие обратные связи

Свойства LSFR:

1. Период выходной последовательности $T<=2^n-$
2. Максимальный период (2^n-1) достигается если ЛРР основан на примитивном полиноме:
   - Примитивный полином
     - неприводимый – не представим в виде произведения полиномов меньшей степени.
     - делит X^k+1, где $k = 2^{n-1}$, но не делит X^d+1 для любого d, такого, что d делит 2^{n-1}
   - Примитивные полиномы существуют для всех степеней. Существуют методы, позволяющие проверить на примитивность произвольный полином.

3. Выходная последовательность ЛРР, основанного на примитивном полиноме обладает свойствами:
   - баланса – равенство количество нулей и единиц (единиц на одну больше)
   - окна – выходная последовательность содержит все возможные варианты заполнения регистров (кроме нулевого) по одному разу.

Свойство окна

- 110
- 101
- 111
- 001
- 011
- 010
- 001
- 110101111001011010001110101111001011010001

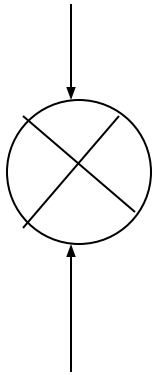
Недостаток генератора Г на основе ЛРР

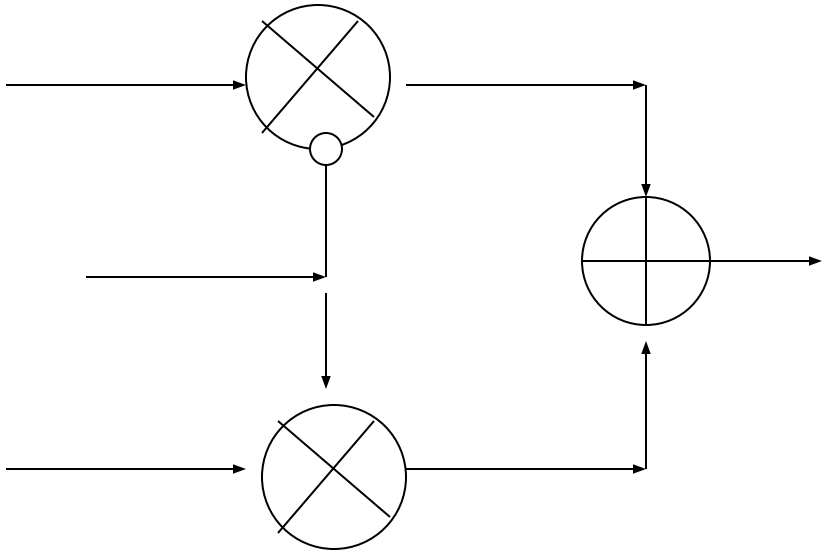
- Непосредственно использовать ЛРР для шифрования нельзя, так как существует алгоритм (Месси-Берликампа), который по 2n символам выходной последовательности восстанавливает вид обратных связей и начальное заполнение. Сложность алгоритма ~n^3
  n – длина регистра сдвига.

- Полиномиальная сложность восстановления регистра по выходной последовательности обусловлена его линейностью.
- Для устранения данного недостатка в схему формирования Г вводят нелинейные элементы

НУУ (нелинейные узлы усложнения)

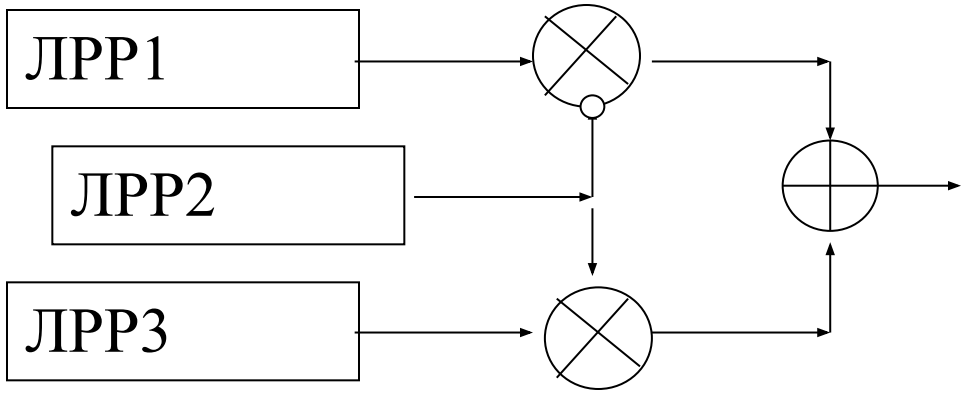
- Схема И Генератор Джеффа(Гефа)

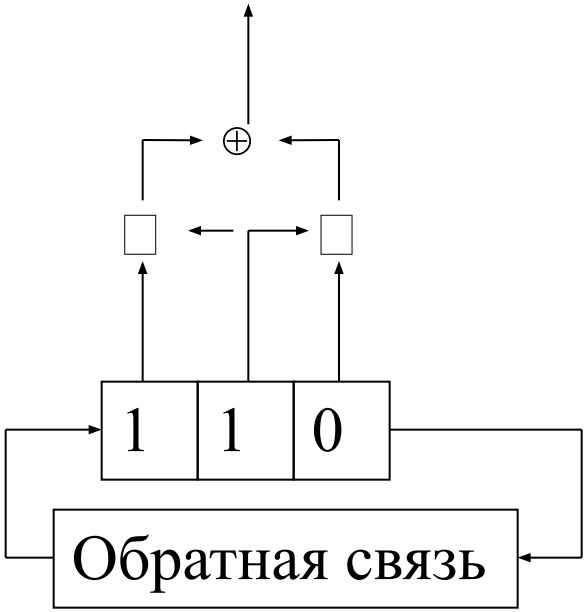




Ввод нелинейности

(комбинация методов)





Управление тактовыми импульсами.

Один LSFR (ЛРР) управляет тактированием другого …

Эквивалентный регистр

- Любой совокупности ЛРР и НУУ можно сопоставить один эквивалентный ЛРР большей длины.

$$d_{экв} >> \sum_{i} d_{ЛРР(i)}$$

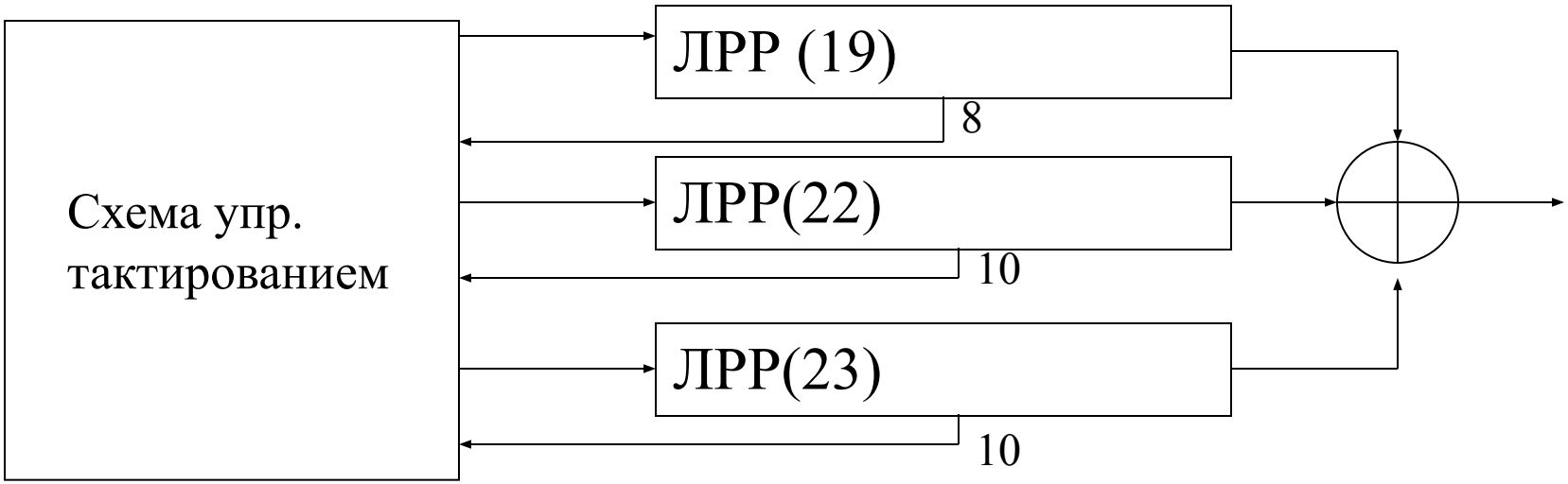
Свойства потоковых шифров*

- Простота схем и низкая стоимость
- Высокая скорость
- Нет размножения ошибок
- Нет задержек
- Проще оценивается стойкость.

* - по сравнению с блоковыми

Примеры потоковых шифров

- A5 (шифрование в GSM)



Особенности A5 (недостатки)

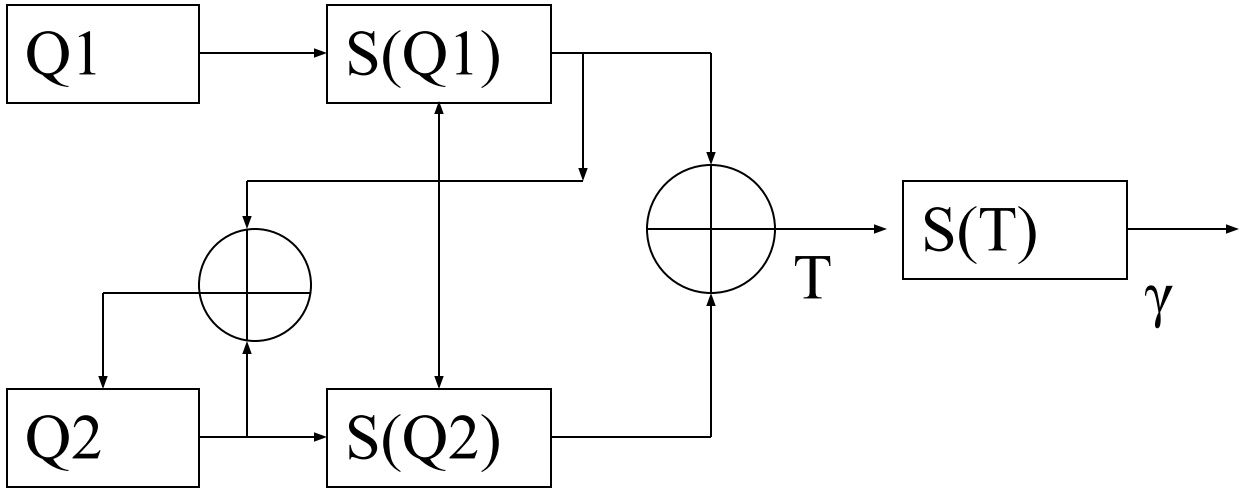
- Первоначально секретный алгоритм
  - A5/1 $\sim 2^{40}$ *
  - A5/2 менее стойкий $\sim 2^{18}$ *

* - при атаке по известной гамме.

- Полиномы обратных связей разрежены (для упрощения аппаратной реализации, но при этом несколько снижается стойкость.)
- Шифруются данные только между абонентом и базовой станцией.

RC4

- Ривест (Райвест):



- Q_1 Q_2 – счетчики – для постоянного изменения таблицы замен.
- S( ) – блоки замены
- Сумматоры по модулю 2^8

RC4

- $Q_1=(Q_1+1) \bmod 2^8$
- $Q_2=(Q_2+S[Q_1]) \bmod 2^8$
- $S[Q_1]$ <--> $S[Q_2]$ - обмен значениями
- $T= (S[Q_1]+S[Q_2]) \bmod 2^8$
- $\gamma = S[T];$

- Для работы алгоритмы необходима первоначальная инициализация таблиц замен.

Другие потоковые шифры

- SEAL (Software-Optimized encription Algorithm)
  - Авторы: Ф. Рогуэй, Д. Копперсмит
- CHAMELEON
  - Автор: Р.Андерсон
- SOBER
  - быстродействие. Для шифрования речи.
- …